Santorini GR

DTIS Design & Technology of Integrated Systems In Nanoscale Era 2014

May 6-8, 2014

Towards Resilient Cyber-Physical Systems:

The ADREAM Project

Jean Arlat

[jean.arlat@laas.fr]

Michel Diaz and Mohamed Kaâniche

LAAS-CNRS

INSTITUT CARNOT LAAS CNRS

www.laas.fr

cnrs dépasser les frontières

Université de Toulouse

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

Tomorrow’s is (almost) Here Today

Some Perspectives

- **Emerging Services and Trends**
  - **Guidance in Public space**
  - **Assistance to Elderly people,…**
  - ***Unmanned* search, Rescue and Recovery**
  - **Smart Grids for Heterogeneous and Distributed “supply chain”: control, monitoring and metering**
  - **Car *and* Home Energy Management**
  - **Autonomous Individual Vehicles Systems, On-demand transportation**
  - **Factory of the Future (Workshop with Humans and Robot Co-workers)**
- **Integration of Information Processing into Everyday Objects and Activities**
  - **Harware and Software Technologies Development**
  - **Interconnection and Communication Capabilities**

Context, Rationale and Challenges

- Trend
  - Massive Deployment of Autonomous “Smart” Objects
  - From Ubiquitous Sensors to Fleets of Service Robots
- Perspectives
  - More hospitable and sustainable future
  - More efficient management of our environment: homes, work places, public areas, etc.
- Features and Issues
  - Management of “COTS” Equipments and Innovative Wireless Communicating and Interdependent Objects
  - Heterogeneity, Scalability, Mobility, Evolutivity,
  - Interoperability, Acceptability, Privacy, Resilience

From Embedded Systems (ES) to Cyber-Physical Systems (CPS)

- Embedded System: a computerized system with a dedicated function within a larger system, often characterized by real-time computing constraints

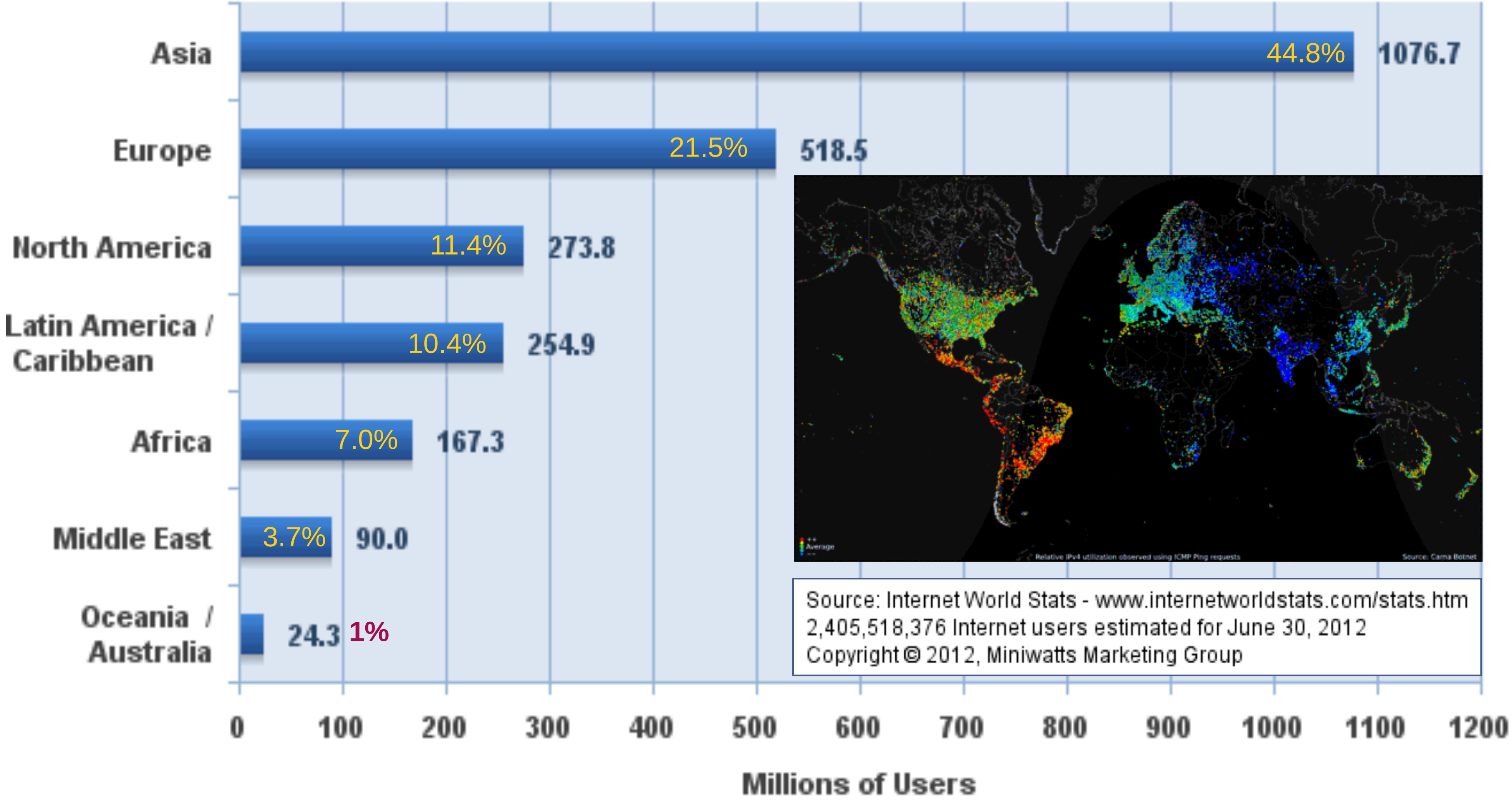
  ES are commonly found in many industrial, transportation, medical, commercial and military applications…

- Cyber-Physical System: "ES" with augmented features
  - Tight Interaction and Coordination between computational and physical resources: Intensive sensing, Smart sensors,…
  - Openess, Pervasiveness: Communication, Mobility,…
  - Large set of Data: Processing, Fusion , Decision/Optimization,…
  - Autonomy: "all-in-one" (monitoring-decision-control) systems: Robots
  - Dependence and Human issues: strong requirements on dependability, security, acceptability/privacy and resilience

➔ Ubiquitous computing, Ambient intelligence, Internet of things…

Internet Usage - Worldwide

World Population: 7,017,846,922
Users: 2,405,518,376
% Penetration: 34.3 %
% Growth (wrt 2000): 566.4 %
June 30, 2012

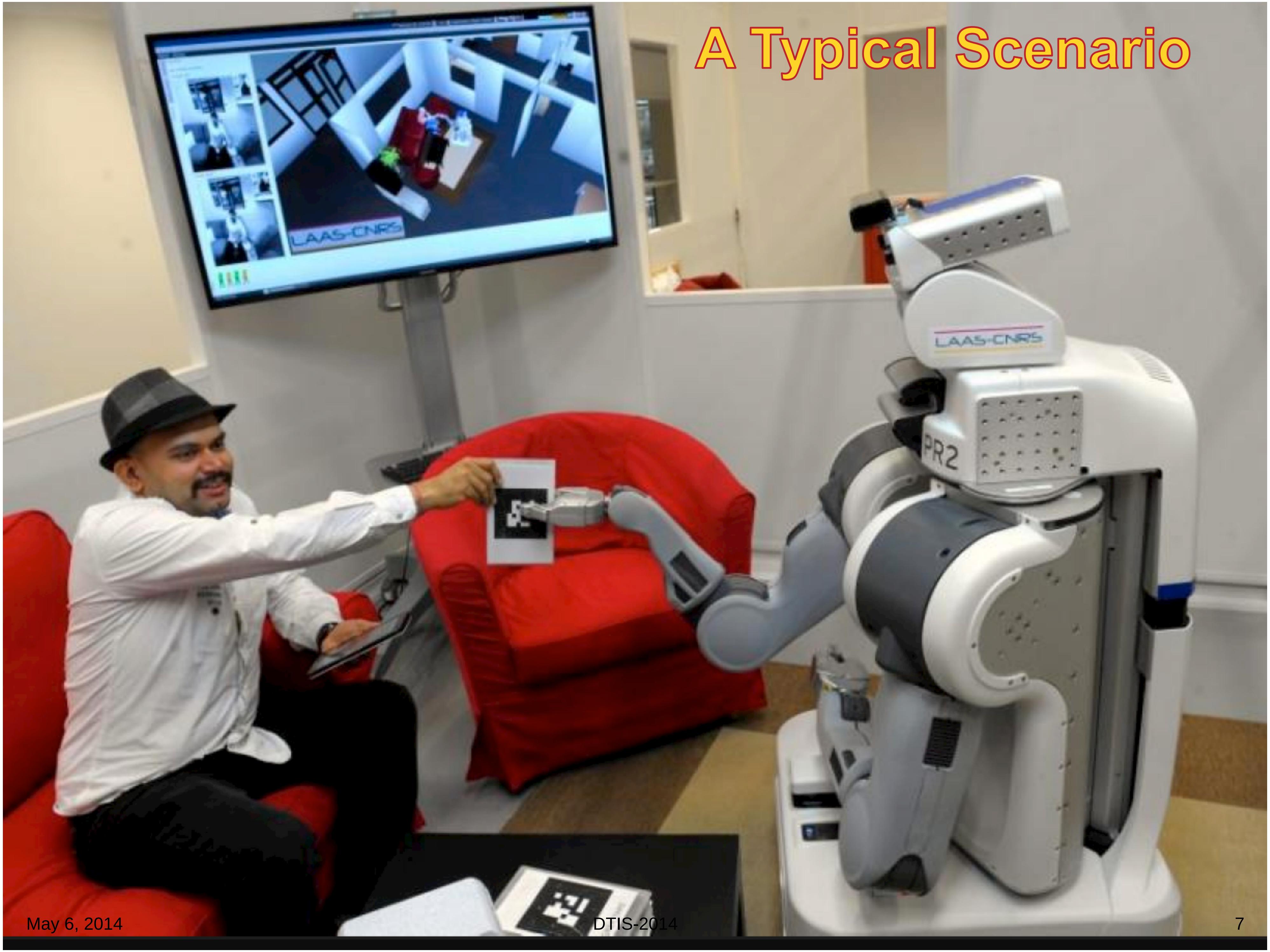


Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

IoT would encode **50 to 100 trillion** objects and be able to follow their movements!

Human being (in urban environment), surrounded by **≈1000-5000** trackable objects

A Typical Scenario



Cyber-Physical Systems

Threats

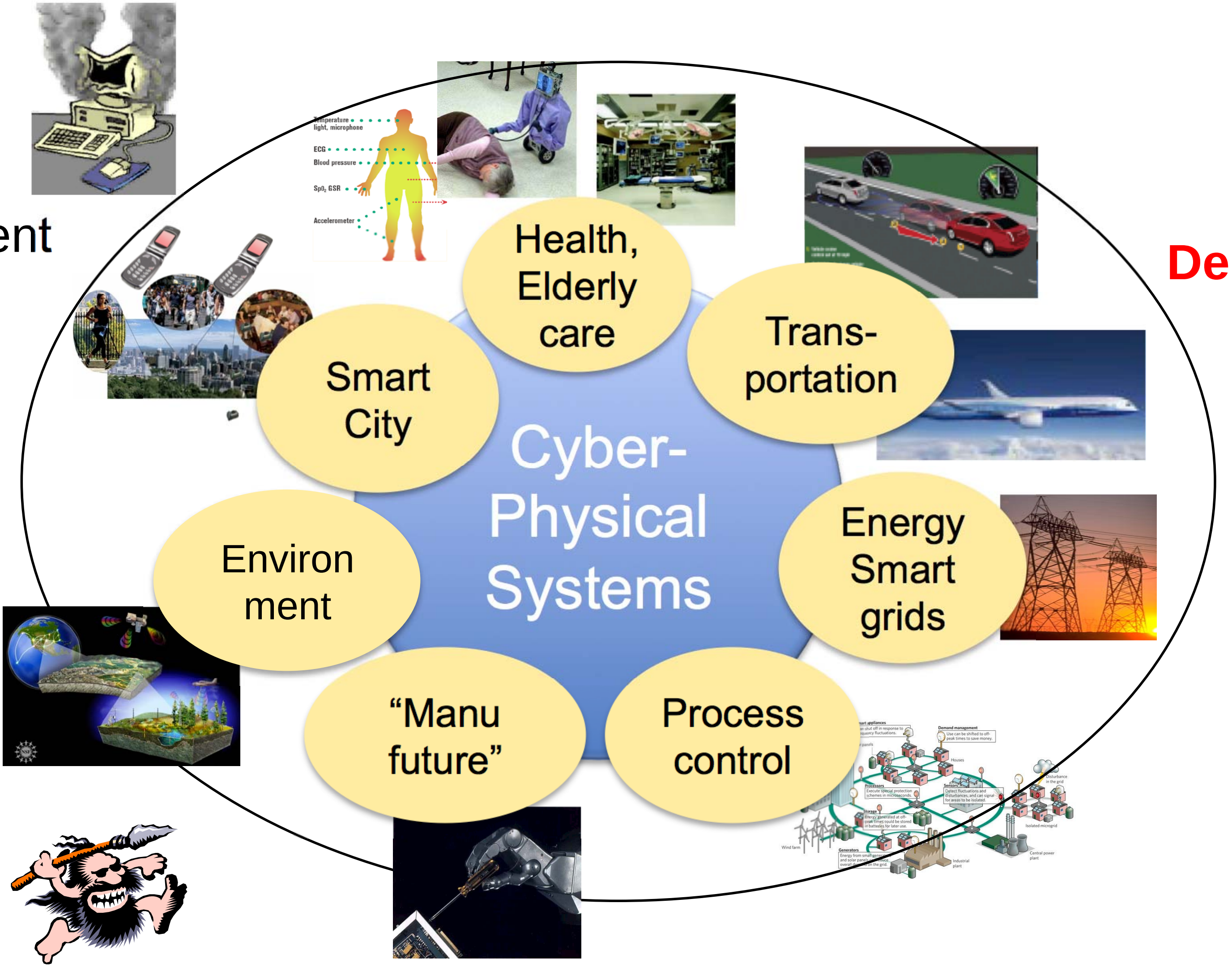
Metrics

Physical faults

Development (HW, SW) faults

Non malicious Human-interaction errors

Malicious Interaction faults



Dependability

Security

…

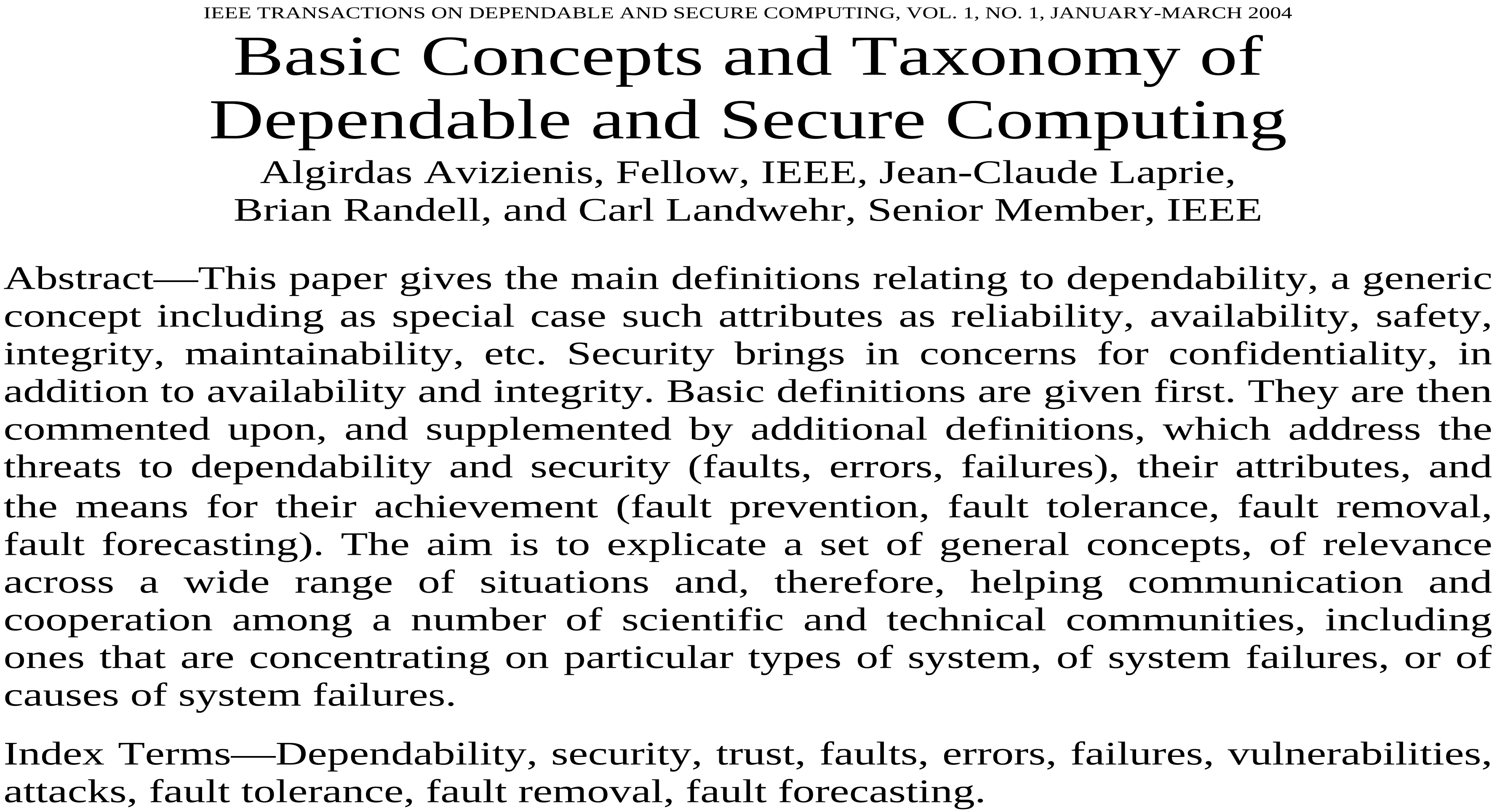
Resilience

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

Basic Concepts

IFIP WG 10.4: Dependable Computing and Fault Tolerance



IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004

Basic Concepts and Taxonomy of Dependable and Secure Computing

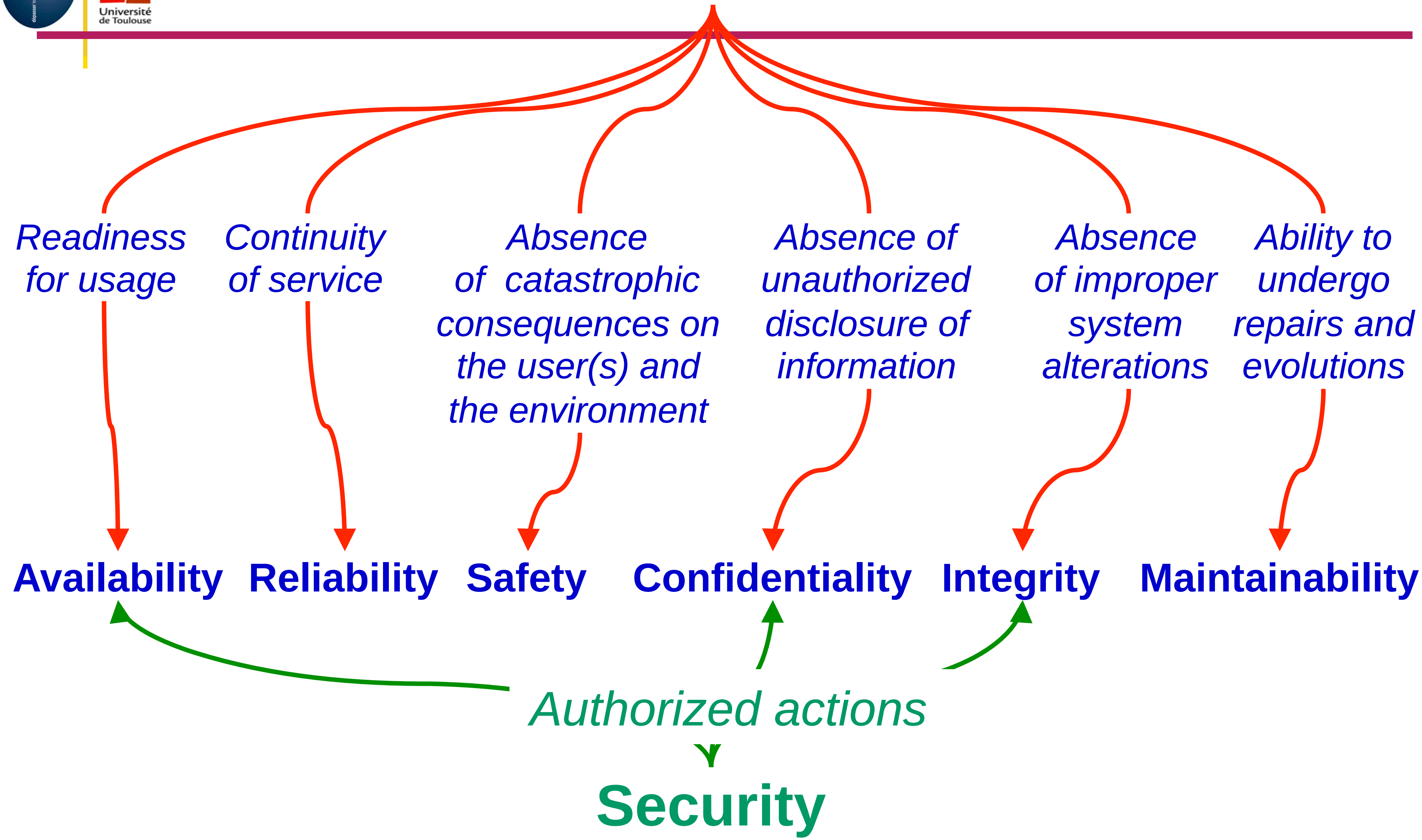
Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie,
Brian Randell, and Carl Landwehr, Senior Member, IEEE

Abstract—This paper gives the main definitions relating to dependability, a generic concept including as special case such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting). The aim is to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures.

Index Terms—Dependability, security, trust, faults, errors, failures, vulnerabilities, attacks, fault tolerance, fault removal, fault forecasting.

IEEE Transactions on Dependable and Secure Systems, Vol. 1, n° 1, 2004

About Dependability



Readiness for usage

Availability

Continuity of service

Reliability

Absence of catastrophic consequences on the user(s) and the environment

Safety

Absence of unauthorized disclosure of information

Confidentiality

Absence of improper system alterations

Integrity

Ability to undergo repairs and evolutions

Maintainability

Authorized actions

Security

Absence of unauthorized access to, or handling of, system state

The Notion of Resilience*

- **Dependability: The ability to deliver a service that can justifiably be trusted**

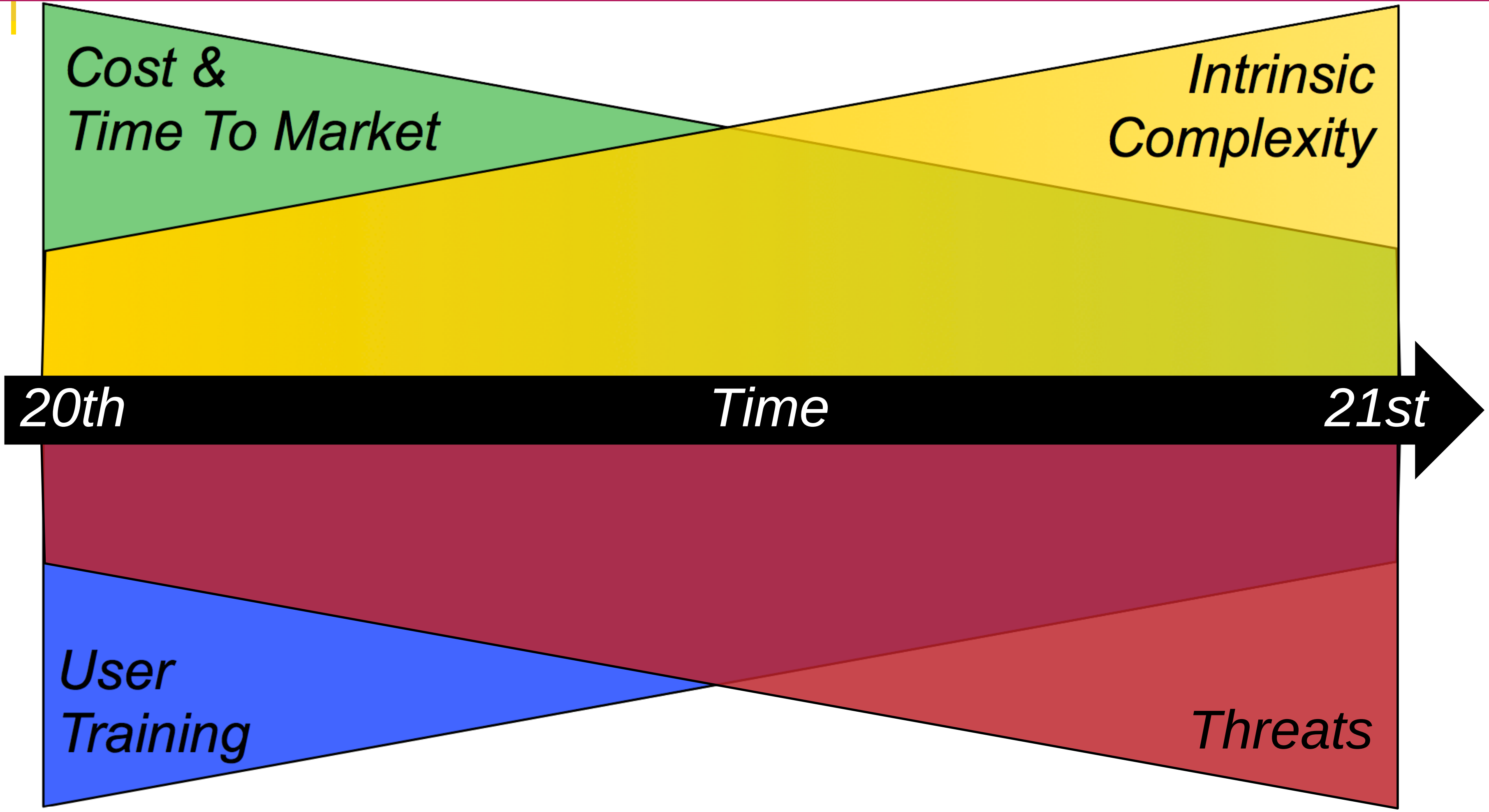
- **Resilience: The persistence of service delivery that can justifiably be trusted, when facing changes**

➔ **The persistence of dependability when facing changes**

Why is this essential ?

*** J.-C. Laprie**
From Dependability to Resilience
Fast Abstracts Session, IEEE/IFIP DSN, Anchorage, AK, USA, June 2008

Looking Ahead: An Ever Moving Target

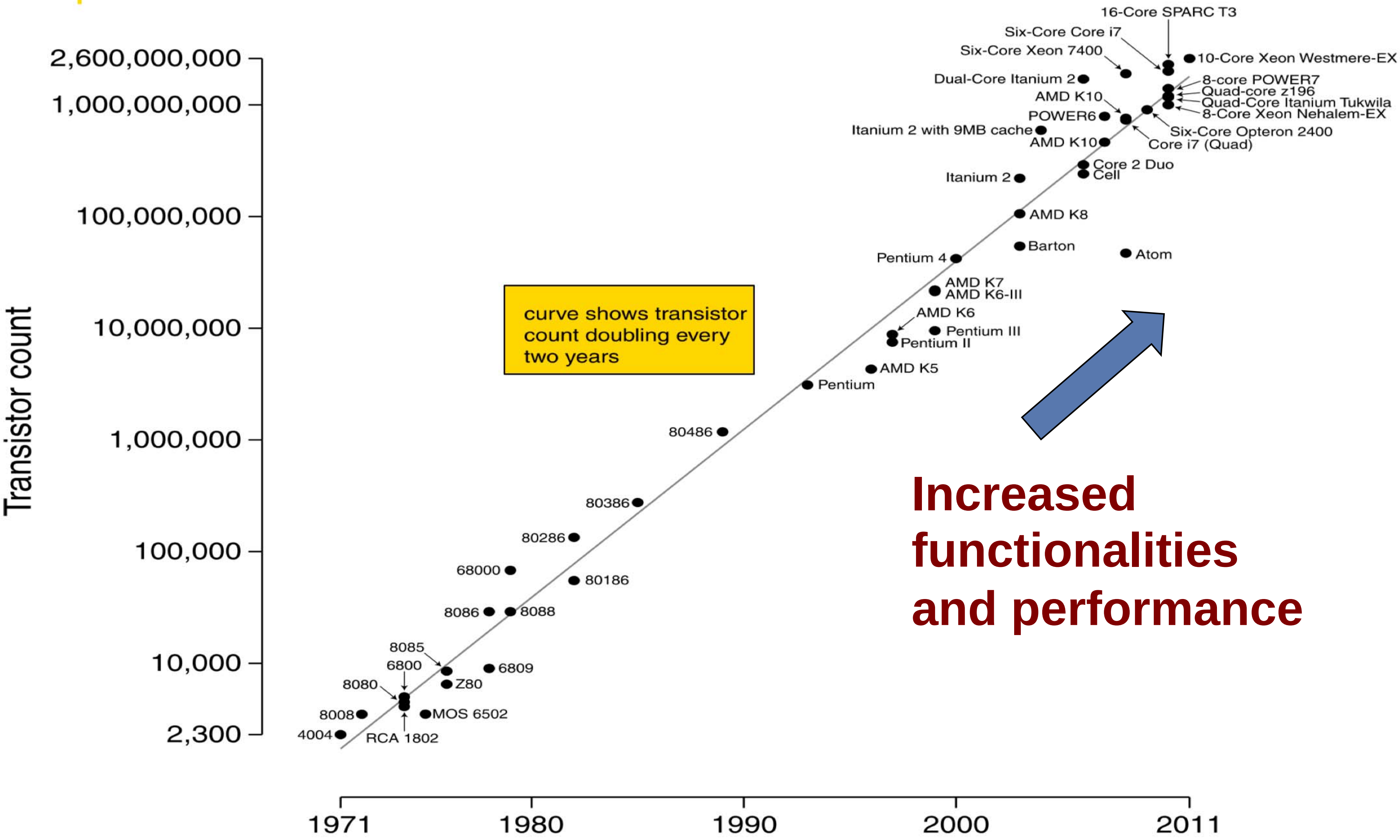


See also:
D. Siewiorek, R. Chillarege, Z. Kalbarczyk
Reflections on Industry Trends and Experimental Research in Dependability
IEEE TDSC, Vol. 1, No. 2, April-june 2004, pp. 109-127

Characteristics & Challenges

- **Evolvability/mobility**
  - Changing environment, topologies, connectivity characteristics, threats
- **Autonomy**
  - Autonomy of decision, power, …
  - Accurate sensing and perception of the environment
- **Complexity**
  - Systems of Systems
  - Large scale deployment
  - Heterogeneity
  - Big Data

The “Moore’s Law” Trend



Increased functionalities and performance

Trend in Hardware

Enhanced functionality and performance, definitely a “booster” …, but:
➔ Device size ↘ nanoscale

- **Manufacturing:** Process variations ↗; Costs (lithography, testing) ↗; Yield ↘ ; Prob. defects get undetected ↗ ; Impact of defects ↗
- **Operation:** Frequency ↗; Power dissipation ↗; Parameter variation ↗; Power supply voltage ↘; Soft Error Rate ↗
- **Correctness ↘**; **Testability ↘**; **Robustness ↘ !?**

From: **100% Reliability**
To: **100% Dependability/Resilience**

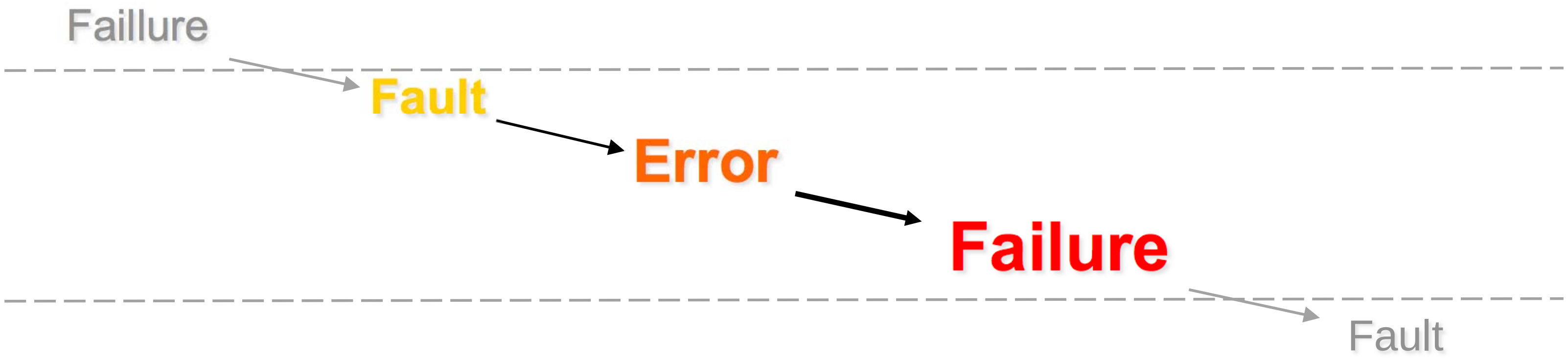
International Technology Roadmap for Semiconductors

- **Crosscutting Challenge 5: Reliability (2008 Update)**
  Reliability & Resilience (2009 Edition)
- **2011 Edition/ 2012 Update: Design for Reliability and Resilience confirmed as "new long-term *Grand Challenge*"**
  (together with design of concurrent software)

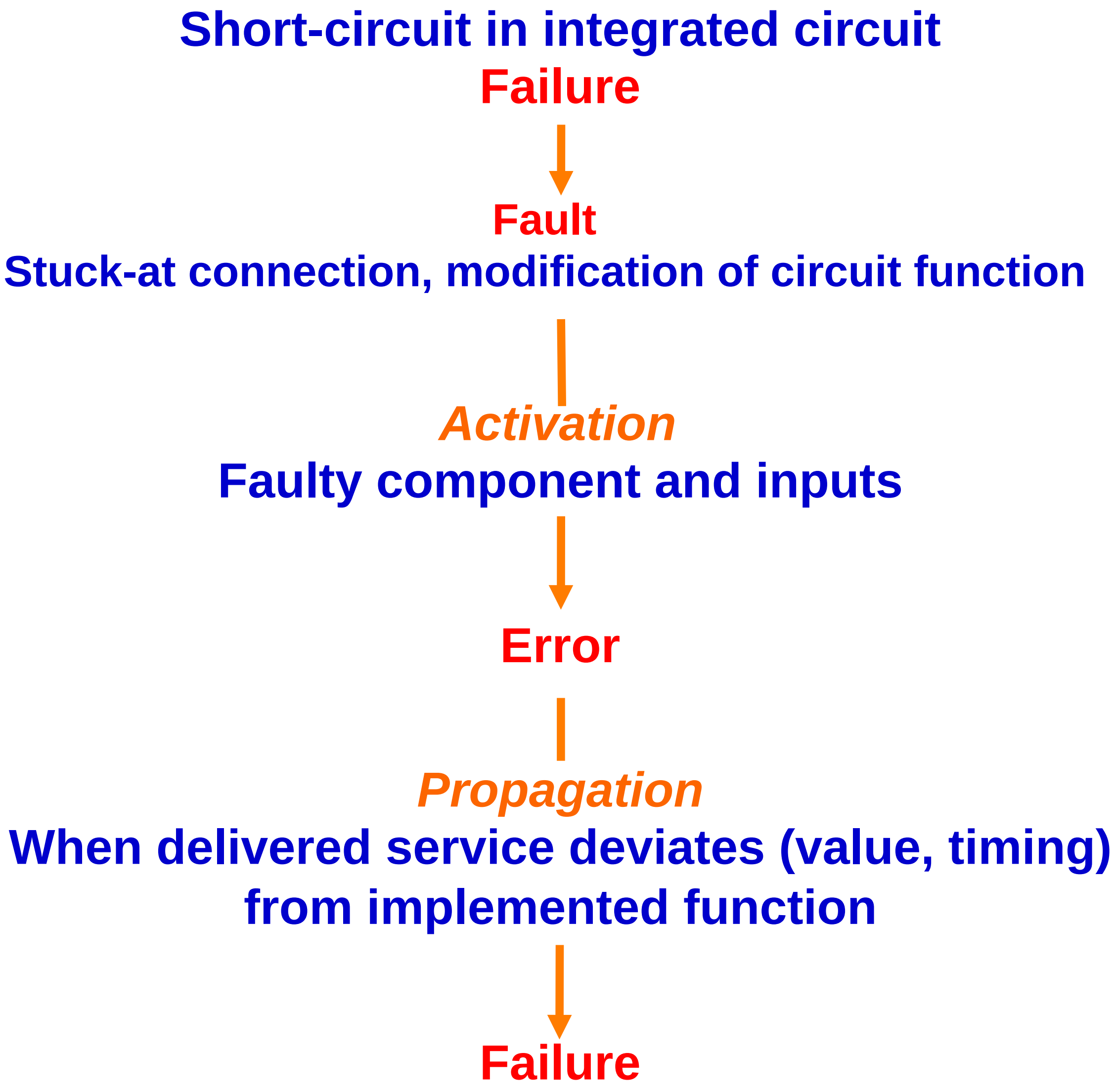
  "Design Technology for Resilience: A Fundamental Portion of DFM"
- **Quoting the Design Section** [http://www.itrs.net/Links/2011ITRS/2011Chapters/2011Design.pdf]
  - ***Relaxing the requirement of 100% correctness for devices and interconnects may dramatically reduce costs of manufacturing, verification, and test***
  - ***Such a paradigm shift will likely be forced in any case by technology scaling, which leads to more transient and permanent failures of signals, logic values, devices, and interconnects***
  - ***In general, automatic insertion of robustness into the design will become a priority as systems become too large to be functionally tested at manufacturing exit***
  - ***Potential solutions include automatic introduction of redundant logic and on-chip reconfigurability for fault tolerance, development of adaptive and self-correcting or self-healing circuits, and software-based fault- tolerance***

About Dependability Impairments

- **Failure**
  - **deviation of the service from the accomplishment of the function of the system**
    - ***Function* : what is the system meant for**
- **Error**
  - **part of system state liable to lead to a failure**
    - ***Error affecting the service* : evidence of failure occurrence**
- **Fault**
  - **cause (attributed or supposed) of an error**



Hardware Fault Pathology



Short-circuit in integrated circuit

Failure

Fault

Stuck-at connection, modification of circuit function

Activation

Faulty component and inputs

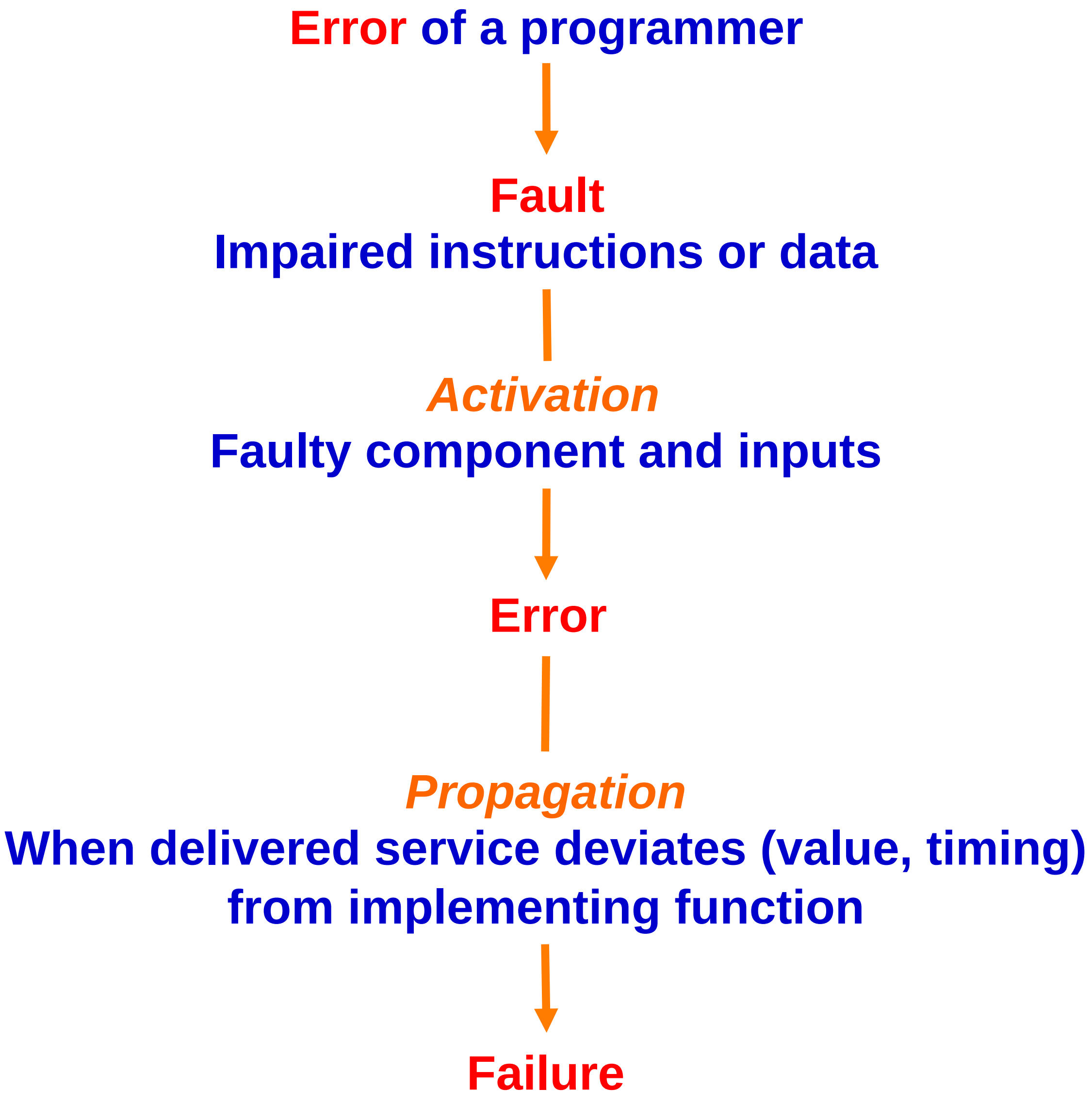
Error

Propagation

When delivered service deviates (value, timing) from implemented function

Failure

Software Fault Pathology



Error of a programmer

Fault

Impaired instructions or data

Activation

Faulty component and inputs

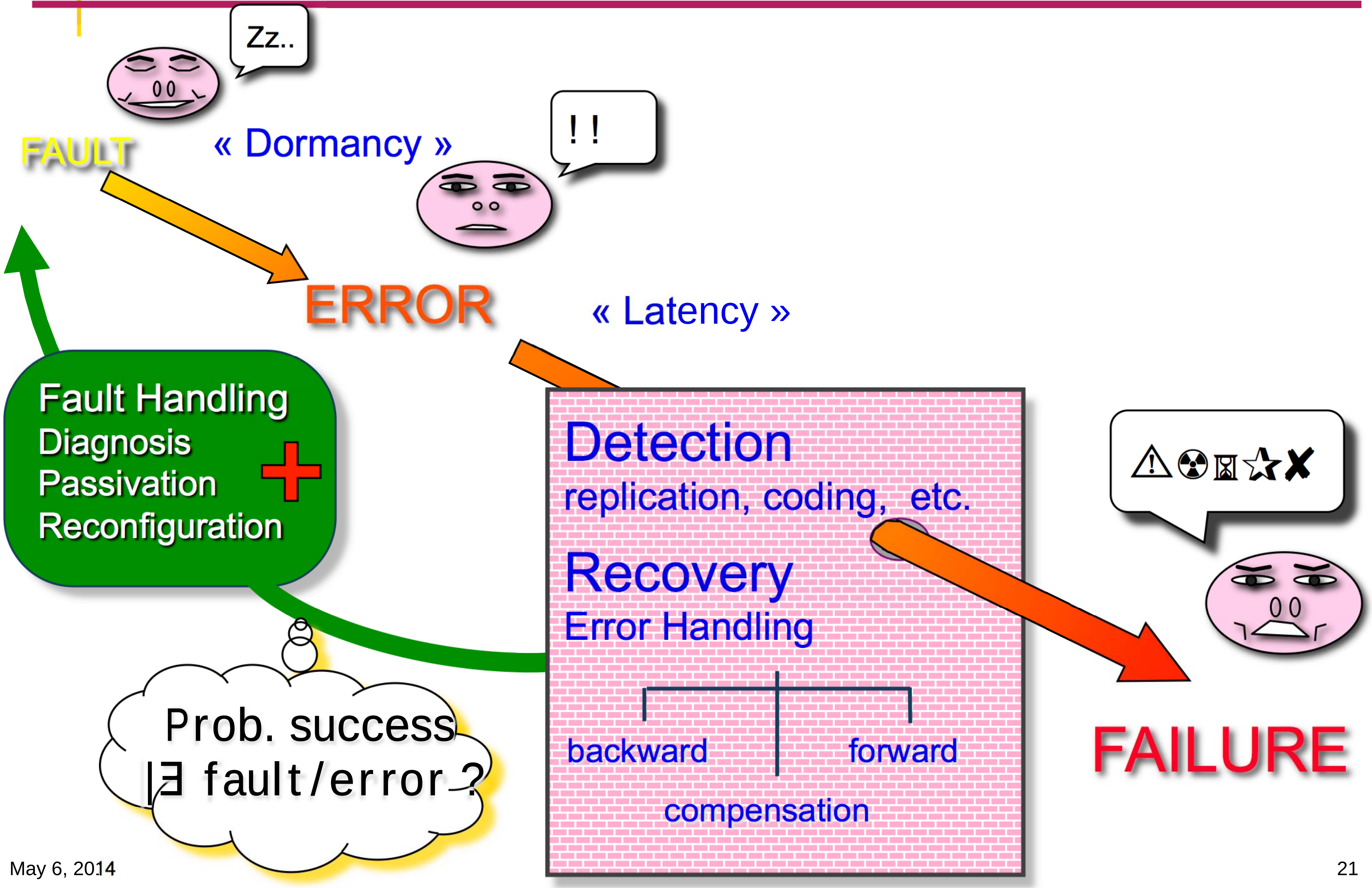
Error

Propagation

When delivered service deviates (value, timing) from implementing function

Failure

Fault Tolerance and Coverage



FAULT

« Dormancy »

ERROR

« Latency »

Fault Handling
Diagnosis
Passivation
Reconfiguration

+

Detection
replication, coding, etc.

Recovery
Error Handling

backward

forward

compensation

FAILURE

Prob. success
|∃ fault/error ?

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

The ADREAM Project

Architectures for Dynamic Resilient Embedded Autonomous Mobile systems

Ambiant Intelligence, Ubiquitous Computing, Internet of Things towards Cyber-Physical Systems

- **Open Networked Embedded Systems, Smart sensors, M2M**
- **Assistance Robots: Companion (Health/Elderly Care), Co-worker (Factory of the Future)**
- **Energy (Harvesting, Conversion, Management, Optimization)**
- **Autonomous Systems and Distributed Control**
- **Rigorous Design, Quality of Service, Resilience, Security, Privacy,…**

Disciplinary Domains, Scientific Themes & ADREAM

Computer Science	• Crucial Computing	(61)
	• Networks and Communications	(59)
Robotics	• Robotics	(80)
Automatic Control	• Decision and optimization	(80)
Micro and Nano Systems	• Microwaves and Optics: From Electromagnetism to Systems	(69)
	• Nano Engineering and Integration	(46)
	• Micro Nano Bio Technologies	(55)
	• Energy Management	(47)

ADREAM

What ADREAM is About?

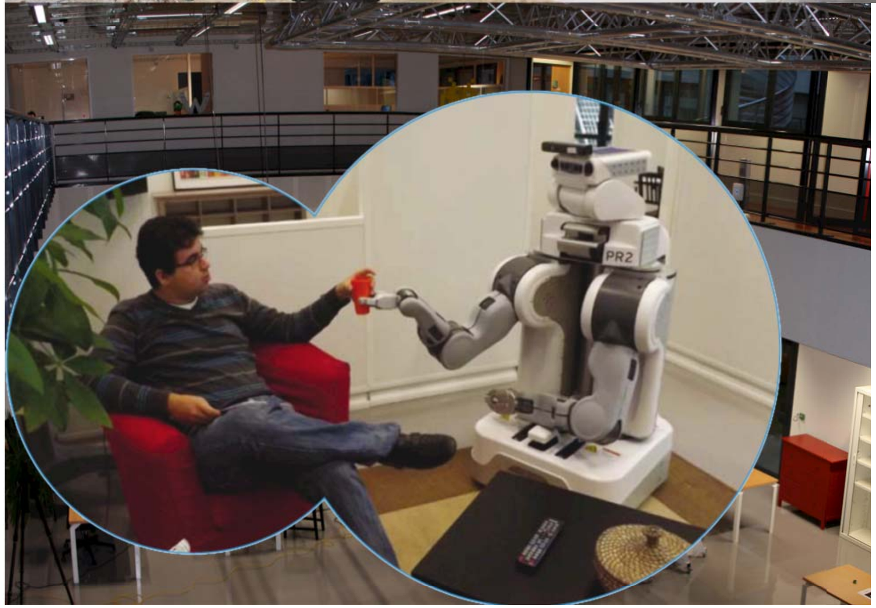
- **A research program: set of coordinated research actions addressing several of the ambitious and interdisciplinary challenges posed by CPS**
- **An experimentation platform: support for the development of most of the ADREAM research actions.**
  - **A new building, fully equipped with sensors, robots, networks, embedded devices, and photovoltaic electricity production facilities**
  - **The platform itself is also the subject of specific research actions involving the set of instrumentation available**

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

The ADREAM Platform @ LAAS-CNRS

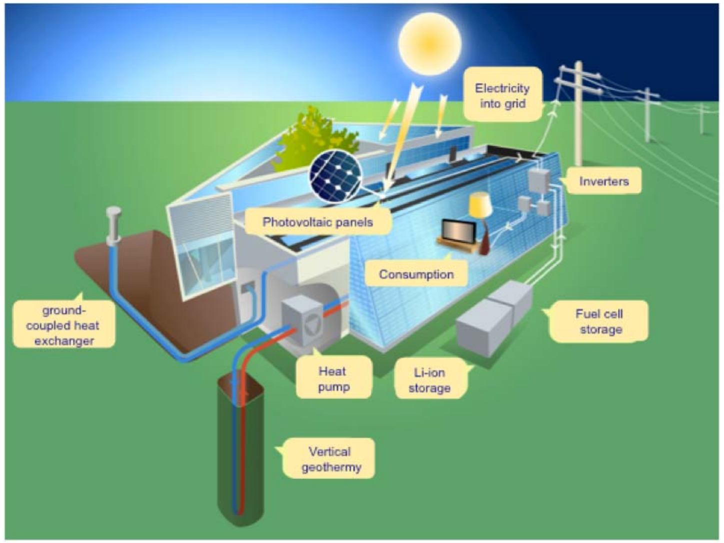
www.laas.fr/ADREAM



- Flexible Experimentation Environnements
- PV Electrical Energy Management
- Sensor Networks
- Robot Fleet (assistance robots, drones)
- Resilience, Quality of Service, Security and Privacy

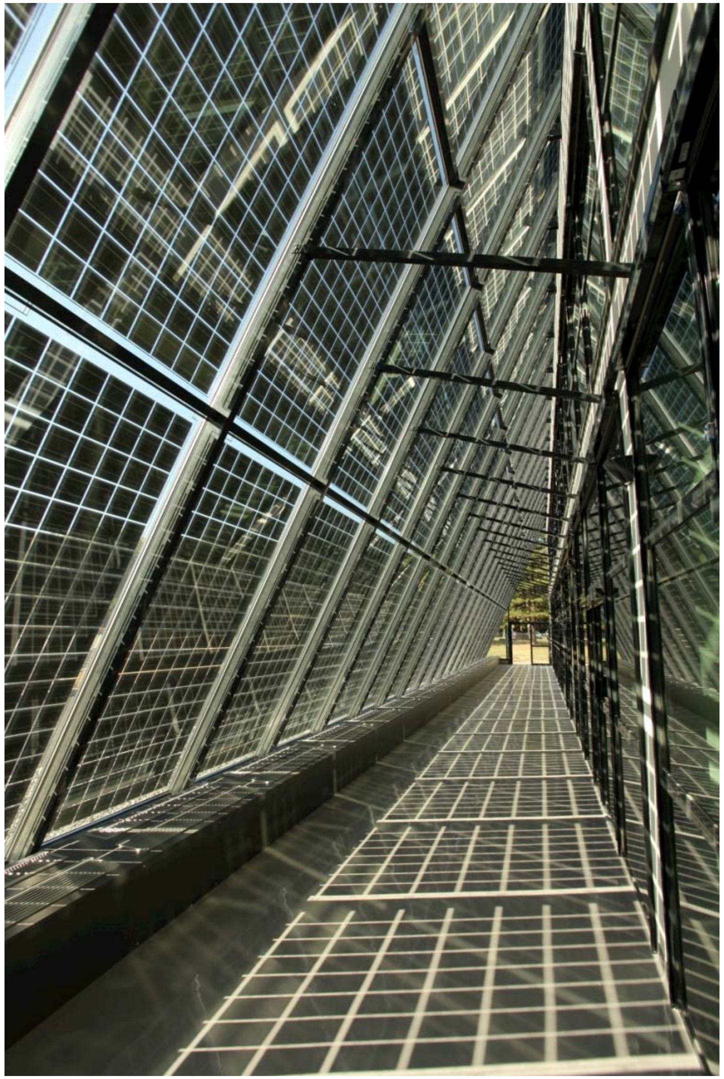
Multi Platform Experimentation Building

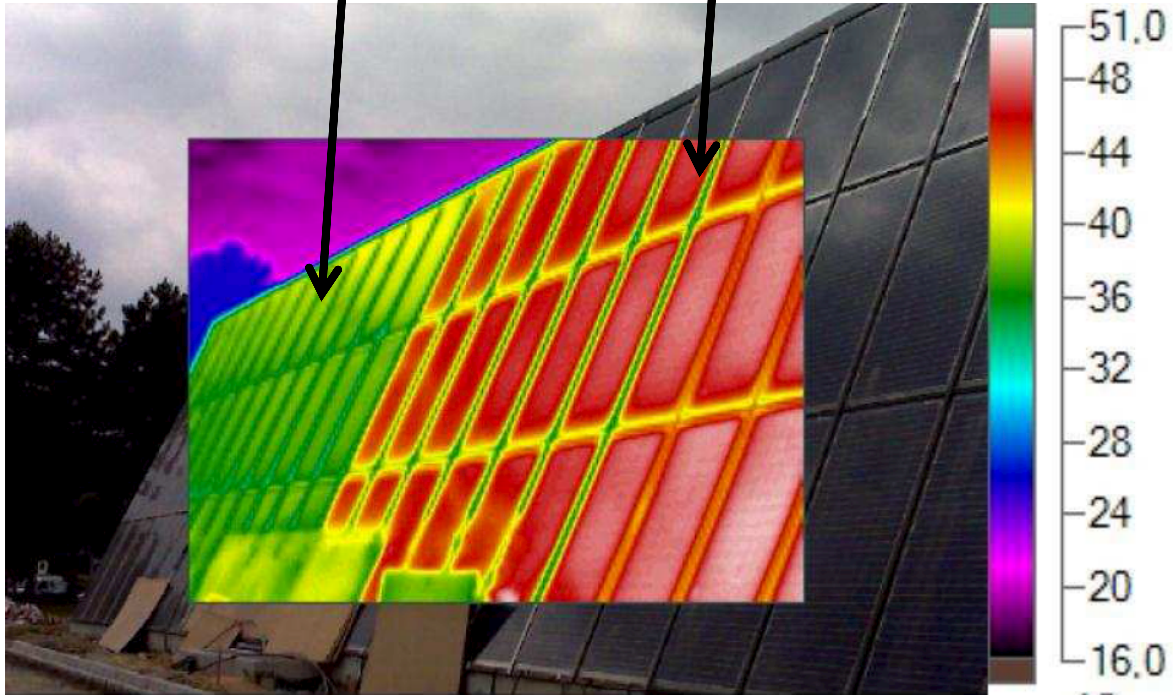
Energy Optimized Building



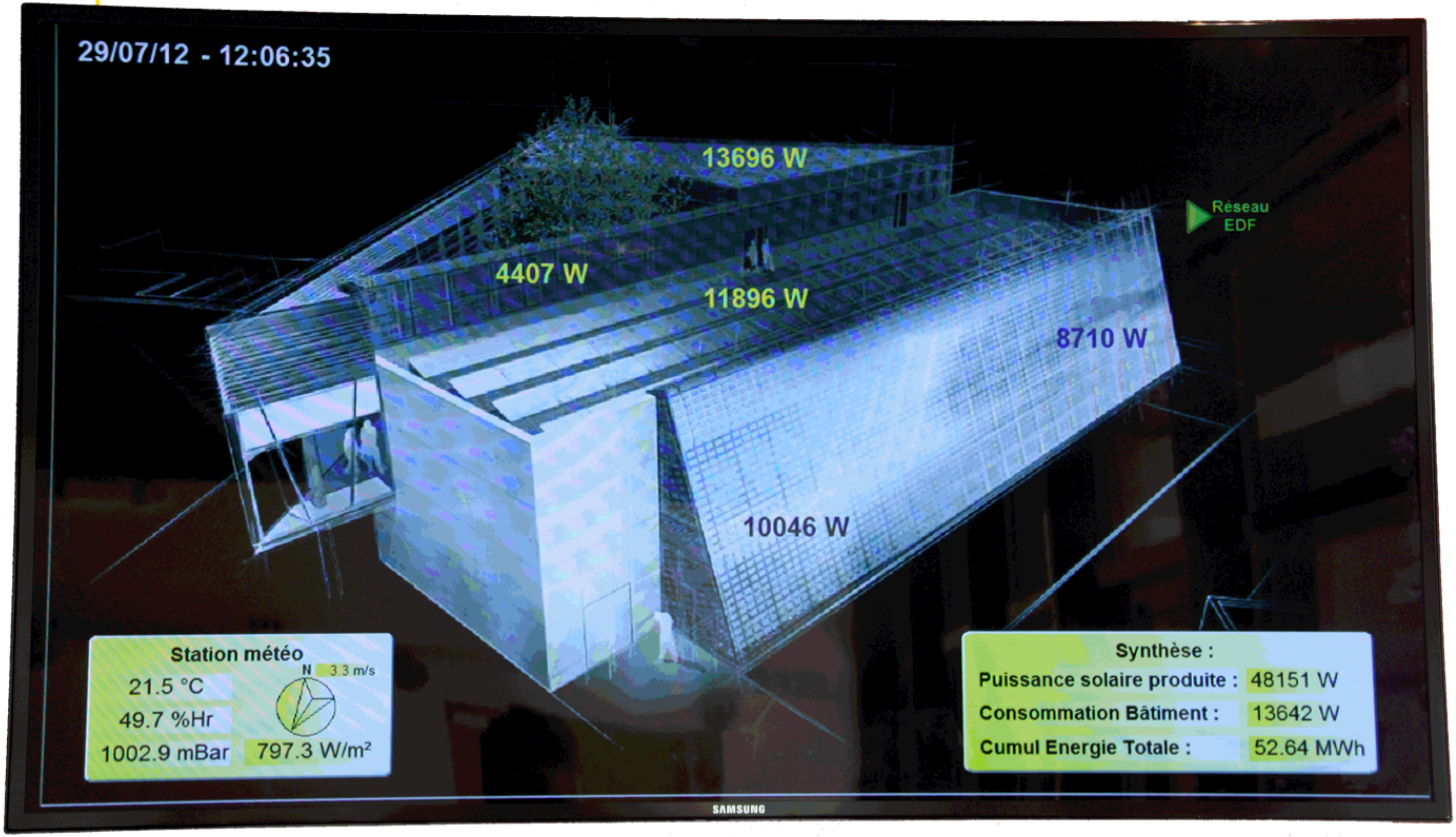
- 500m2 Technical Platforms (IoT, Ambient Intelligence, Energy, Robotics) — 700m2 Offices
- Electricity (500 data collected):
  - consumption (area, usage)
  - Production (photovoltaic)
  - Storage (planned)
- Heating, Air Conditioning, Geothermy, Meteo base (650 measurement and regulation points)
- Lightning (3700 measurement points): Motion, light intensity sensors, regulation per areas according to ambient light, time period, and usage
- Database exploitable for “Big Data” studies

Facade: PV Cells Window-Coating
Dual vs.Triple





Electricity Consumption, Instantaneous & Cumulated PV Production



29/07/12 - 12:06:35

Station météo

21.5 °C

49.7 %Hr

1002.9 mBar

797.3 W/m²

Synthèse :

Puissance solaire produite :	48151 W
Consommation Bâtiment :	13642 W
Cumul Energie Totale :	52.64 MWh

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

The On-going Research Projects

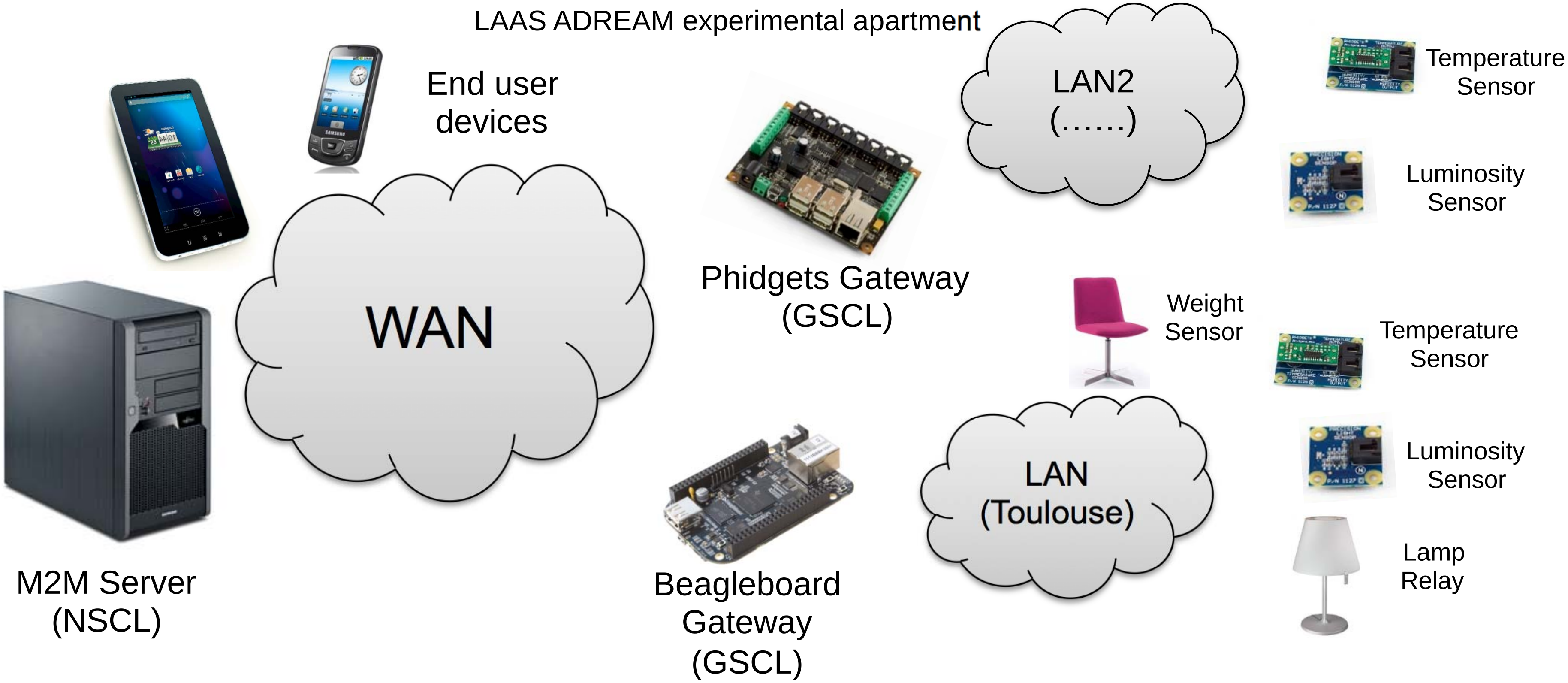
- **Micro and nano sensors**
- **Autonomic ubiquitous computing systems**
- **Localization, navigation, robotics and mobility**
- **Automatic control: distributed and cooperative robust control**
- **Electrical energy management systems and optimization**
- **Security and privacy issues**
- **Formal development and assessment of adaptive mobile systems**
- **System co-simulation and co-validation environments**

Autonomic Ubiquitous Systems

- OM2M
  - First Open Source platform compliant with ETSI Machine to Machine standard for IoT applications [http://om2m.org] (Eclipse License)
  - Implements the functionalities of the layer of ETSI/M2M/ SCL services :
- Various application domains
  - Health/Assistance, Transportation, Domotics, Energy management
- Challenges
  - Adaptive QoS and control of autonomic communications
  - Unsupervised detection of network traffic anomalies

ADREAM – Instrumented “Appartment”

LAAS ADREAM experimental apartment



End user devices

WAN

M2M Server (NSCL)

Phidgets Gateway (GSCL)

Beagleboard Gateway (GSCL)

LAN2 (……)

LAN (Toulouse)

Temperature Sensor

Luminosity Sensor

Weight Sensor

Temperature Sensor

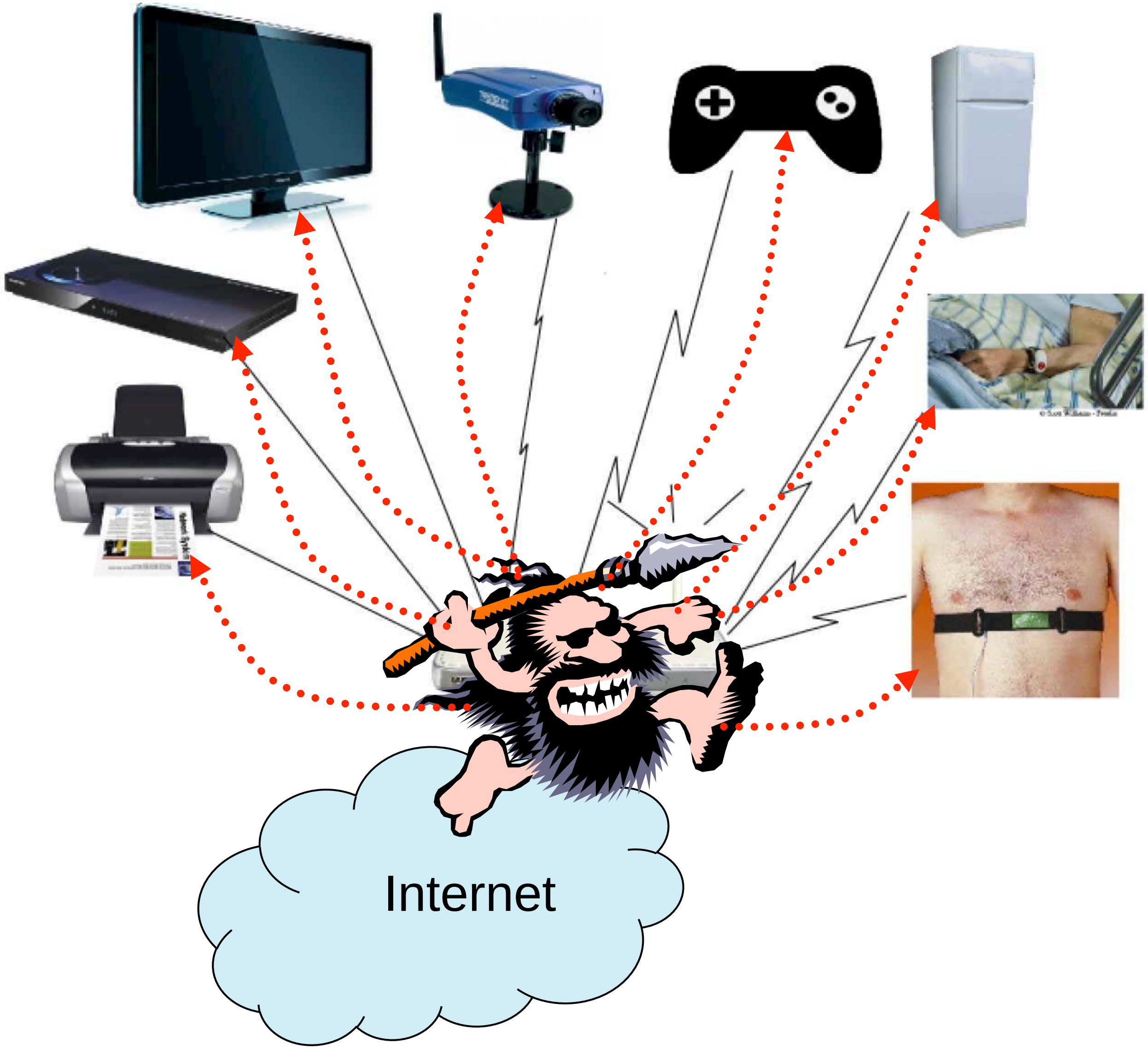
Luminosity Sensor

Lamp Relay

Security

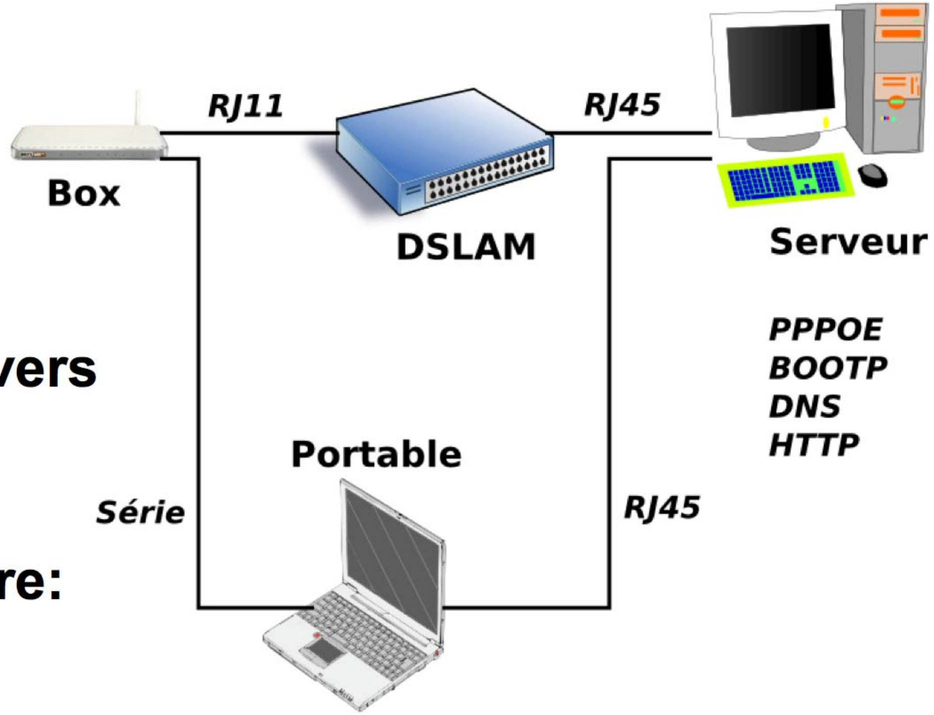
- **First results: ADSL “boxes” are vulnerable**
  - Privilege escalation
  - Box reprogramming to introduce hidden functions (remote control)
- **Other studies**
  - Smart TVs, Google TV (*Thales security*)
  - Embedded systems
    - Automotives (Renault)
    - Avionics, Satellites (AIRBUS, Astrium, …)
  - Assistive robots
  - Medical devices
  - …

Home Networks and Attacks



Security of Consumer Equipments Linked to the Internet

- Comparative study
  - Comparison of the cyphering protocols and mechanisms used by “Box” equipments at startup
  - Identification of vulnerability on a Box
- Exploitation of a vulnerability
  - Principle: Simulate the behavior of “normal” servers of the Box, located on the ISP side
  - Simulation of the normal servers until the remote download of the firmware
  - Download of our own firmware: addition of `telnet` service on the WAN link



On-going Work

- **Internet-linked TV/DVD players**
  - **Misuse of internal functionalities of the equipment, extension of privileges,**
  - **Capabilities for remote exploitation of the equipment**
  - **Input/Output Local Attacks**
  - **Privacy issues…**
- **New Computerized Architectures for Car Vehicles**
  - **Many ECUs communicating via a mutiplexed bus (e.g., CAN)**
  - **So far, attacks seldom considered because a physical connection to the vehicule was necesssary**
  - **Today — several connectivity points**
    - USB and Wireless: Wi, Bluetooth, 3G
  - **Very soon — Extented communications means**
    - V2V (Vehicule to Vehicule) and V2I (Vehicule to Infrastructure)

lefigaro.fr **LE FIGARO**

« Sans la liberté de blâmer, il n'est point d'éloge flatteur » Beaumarchais

Monday

May 5, 2014

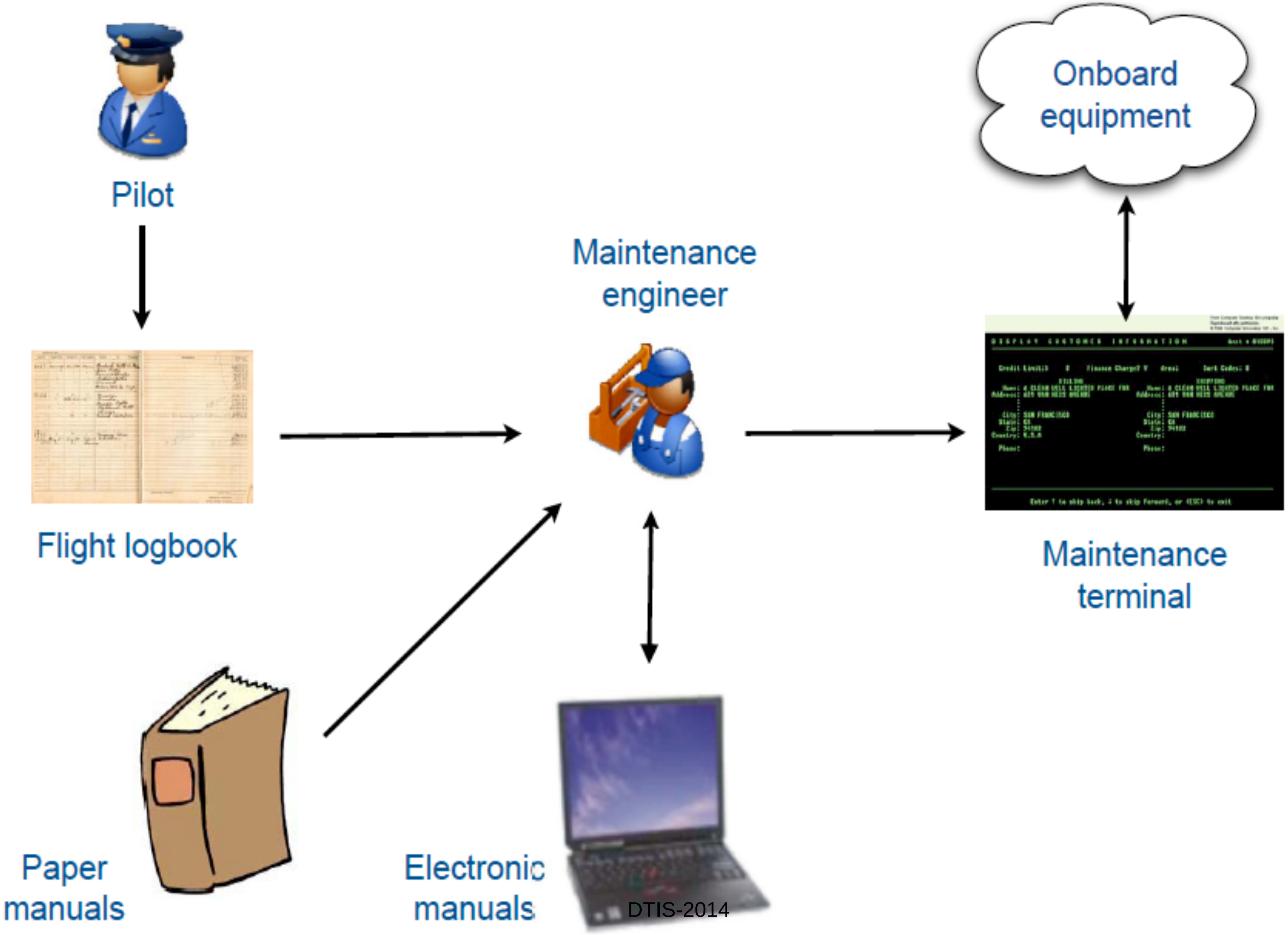
New!

- ***La voiture, nouvelle cible des pirates informatiques***

  The car, the new target for hackers

- **The more cars are embedding electronics, the more they resemble to computers!**
- **The main “entrance”: The OBD (On-Board Diagnostics) connector**
- **The most vulnerable parts: the links between the multimedias functions, the on-line services and the diagnosis tools**
  — that could be used for remotely hacking a car

Aircraft Maintenance: Current Scenario



Pilot

Flight logbook

Maintenance engineer

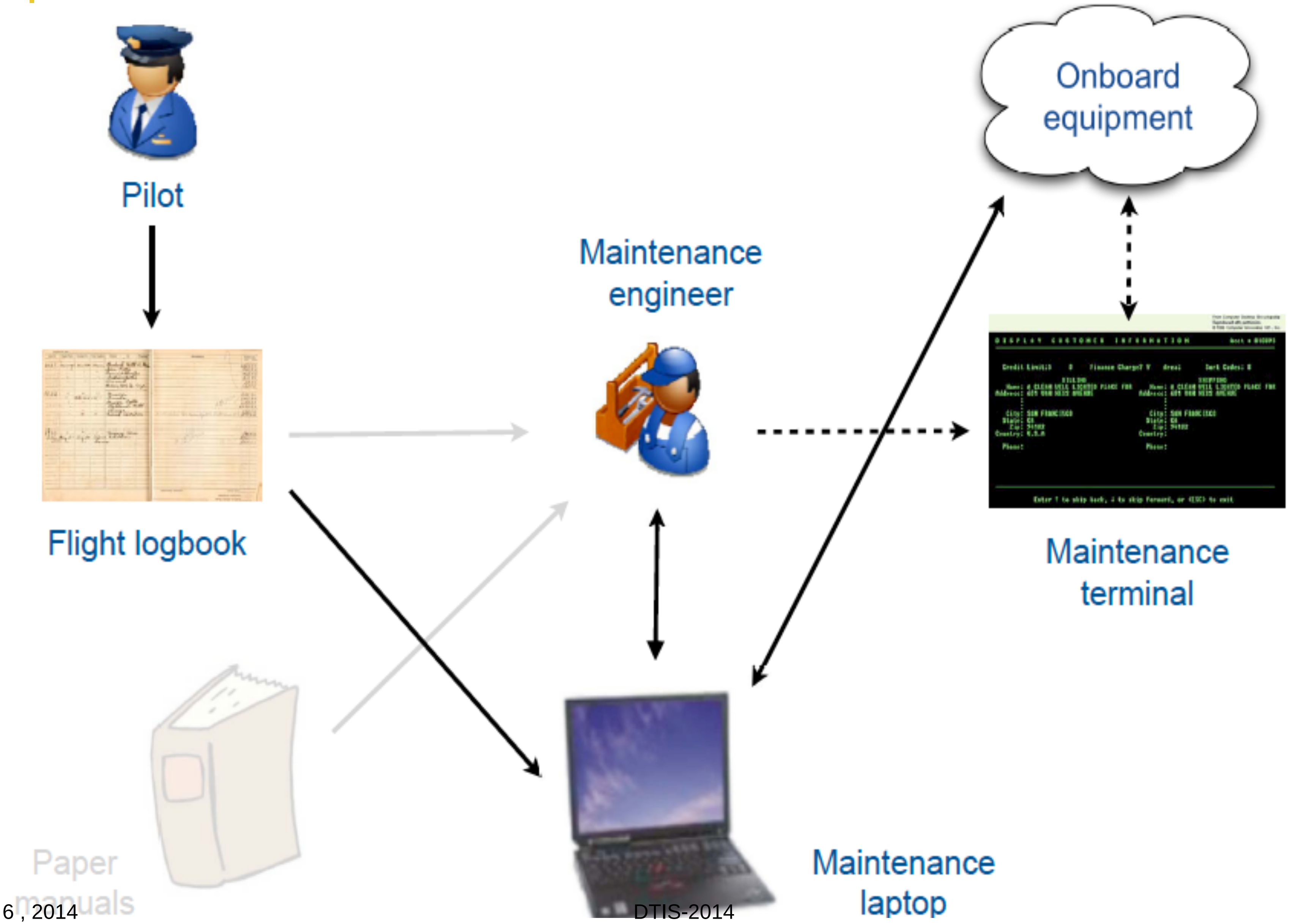
Onboard equipment

Maintenance terminal

Paper manuals

Electronic manuals

Aircraft Maintenance: Laptop Scenario



Pilot

Flight logbook

Paper manuals

Maintenance engineer

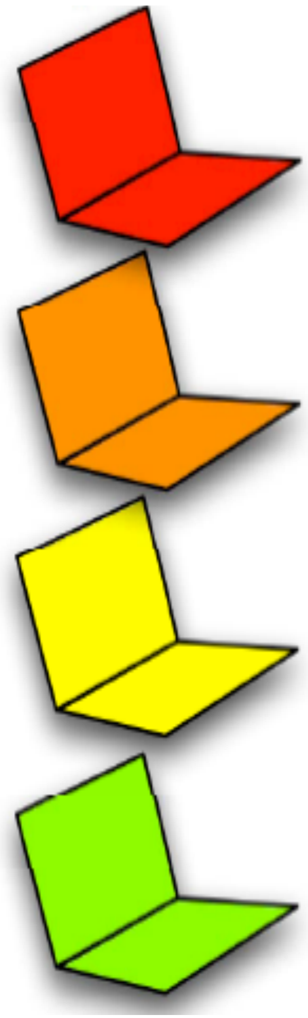
Maintenance laptop

Onboard equipment

Maintenance terminal

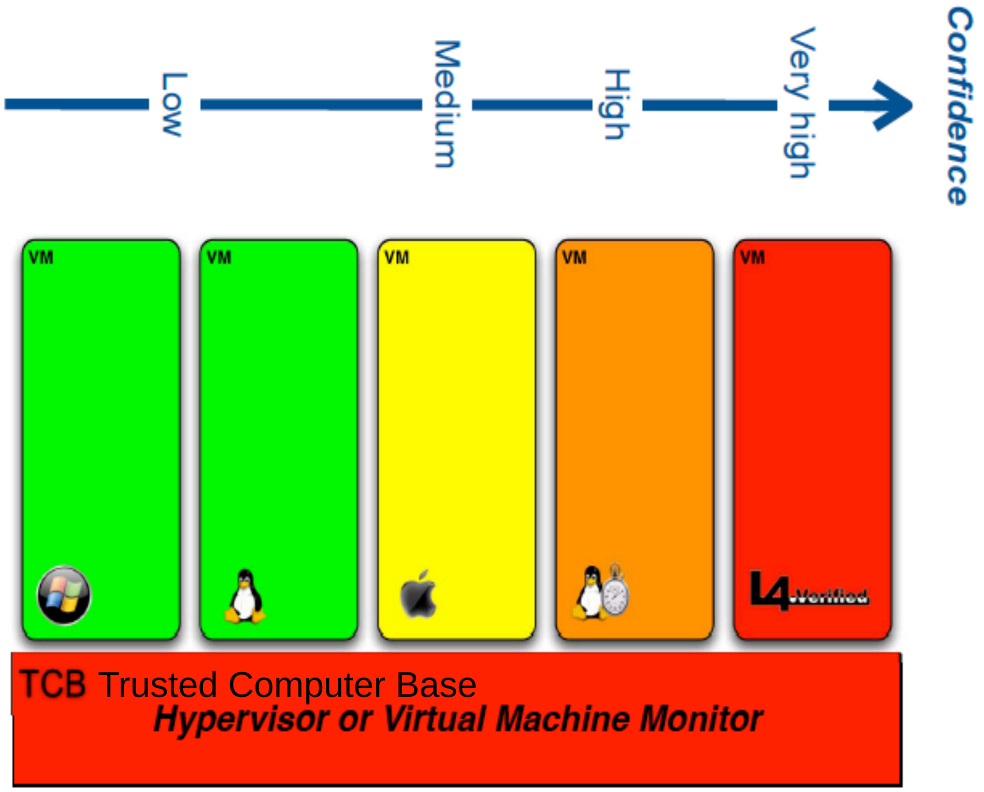
Connecting a Laptop?

Execution confidence	
++	Flight management
++	Aircraft management
+	Aircraft information system
-	"Off-board"

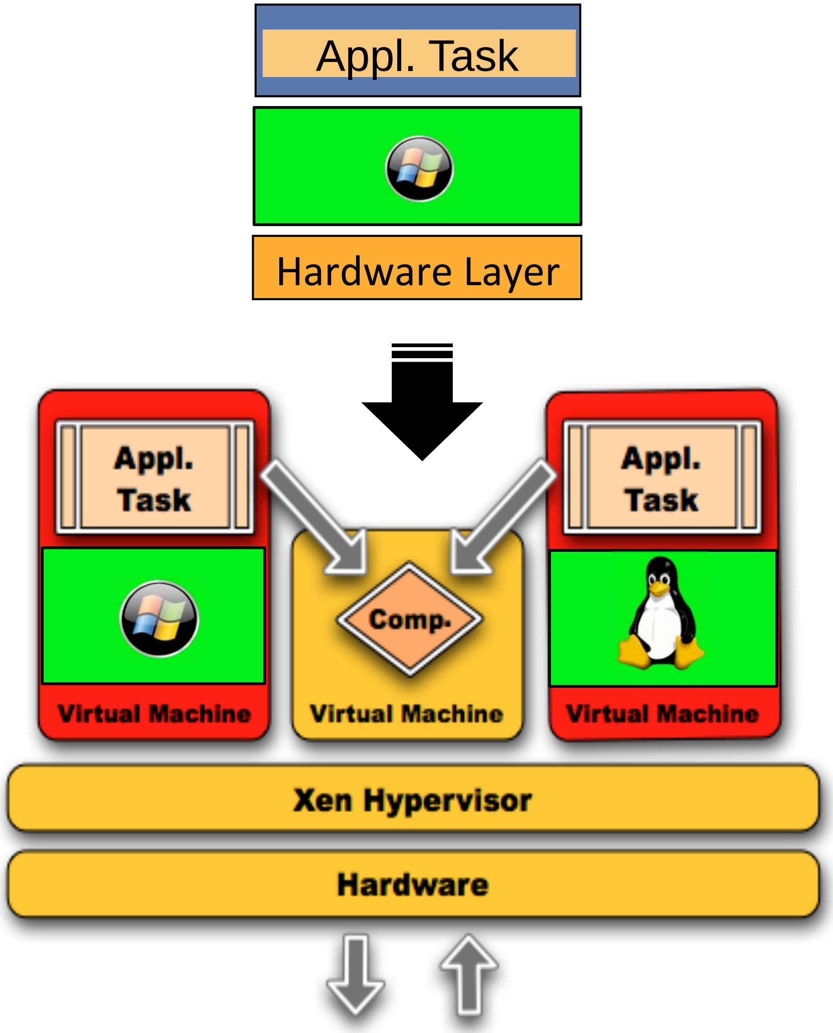


Virtualization for Dependability

Partitioning and Segregation

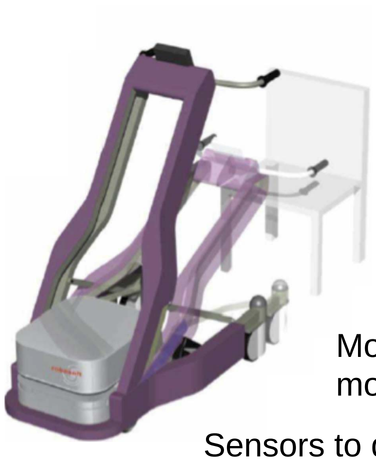

Low
Medium
High
Very high
Confidence
VM
VM
VM
VM
VM
L4.verified
TCB Trusted Computer Base
Hypervisor or Virtual Machine Monitor

Diversified Duplex



Safety Analysis: Autonomous Robot Systems

- **MIRAS : Multimodal Interactive Robot for Assistance in Strolling**
  - Assist patient in standing-up, walking, sitting down
  - People suffering from gait and orientation problems
- **Autonomous Systems & Safety**
  - Complex architectures, human robot interactions
  - Move in an unstructured environment
    - perception uncertainties, non deterministic behavior
- **Goal**
  - Model-based structured approach for safety analysis & argumentation
  - HAZOP-UML based approach
  - Support for the definition of safety monitors



Motorised base & moving handlebar

Sensors to detect patient's position and health condition (heart-rate)

Outline

- Moving Towards a New Paradigm: Cyber-Physical Systems
- From Dependability to Resilience
- The ADREAM Project
- The Supporting Experimentation Platform: Instrumented and Energy-Optimized Building
- The On-going Projects
- Conclusions

Concluding Remarks

- **ADREAM: a rather unique framework and environment to address several of the challenges attached to CPS on a comprehensive basis.**
- **Multidisciplinary approaches become the main focus for the research being conducted:**
  - **development of various types of sensors (e.g., foot/wrist fall detectors), advanced communication devices (highly miniaturized, consumption-free transducers) and low energy, long range communication networks (including M2M layered protocols).**
  - **command-control of a fleet of drones, encompassing complex issues such as: coordinated planning and actions, distributed robust control, algorithm optimization**
  - **control strategy for collecting and processing the data within the instrumented platform for optimizing the control and regulation of the building (temperature, lightning, etc.)**

Perspectives

- **Extend cooperation with other labs and disciplines:**
  - **The energy-related platform from the building is already a shared facility (federation on Energy and Housing)**
  - **The results from the sensor data collection and analysis of the building will benefit the "NeOCampus" project recently initiated on the University campus**
  - **Cross-fertilizing interdisciplinary work: joint consideration of technical, regulatory, economic and social constraints that are attached to the deployment and acceptance of CPS**

Towards Resilient Cyber-Physical Systems:

The ADREAM Project

Thank you!

Jean Arlat

[jean.arlat@laas.fr]

Questions?

Michel Diaz and Mohamed Kaâniche

LAAS-CNRS

INSTITUT CARNOT LAAS CNRS

www.laas.fr

Université de Toulouse